



U.S. Department of Justice

*United States Attorney
Eastern District of California*

*501 I Street, Suite 10-100
Sacramento, California 95814*

*916/554-2700
Fax 916/554-2900*

FOR IMMEDIATE RELEASE
August 12, 2004

*Contact: Patty Pontello, 916-554-2706
www.usdoj.gov/usao/cae/home*

**FORMER VERIZON WIRELESS EMPLOYEE CHARGED WITH STEALING
\$20 MILLION IN PIN NUMBERS FOR PREPAID CELL PHONE SERVICE**

SACRAMENTO--United States Attorney McGregor W. Scott announced today that a federal grand jury returned a 10-count indictment charging TIMOTHY CHARLES MATTOS, 32, of Folsom, California, with fraud and money laundering in connection with his scheme to steal over \$20 million in personal identification numbers ("PINs") for prepaid Verizon Wireless cellular telephone service. Specifically, the indictment charges Mattos with three counts of fraud in connection with computers, five counts of money laundering, and one count of fraud in connection with access devices. In addition, the indictment seeks to forfeit property allegedly derived from the charged crimes.

This case is the product of an investigation by the United States Secret Service with the cooperation of Verizon Wireless.

According to Assistant United States Attorney Norman Wong, who is prosecuting the case, the indictment alleges that Mattos was formerly employed as a customer service representative at Verizon Wireless, a nationwide cellular telephone service provider. Verizon Wireless offered its customers a service plan which allowed customers to prepay Verizon Wireless for cellular telephone service. Verizon Wireless sold prepaid minutes through 15-digit PINs, which were printed on special cards or sold in some other form. To add minutes to their prepaid cellular telephone service accounts, customers could purchase PINs from authorized

Verizon Wireless agents and call a designated telephone number to "activate" the prepaid minutes using an automated system that would credit the proper amounts to the customers' accounts. Verizon Wireless listed available, unused PINs on a customer care website which was not accessible to the general public but required a valid username and password.

The indictment further alleges that as a Verizon Wireless customer service representative, Mattos had access to a valid username and password to log onto the Verizon Wireless customer care website. While employed by Verizon Wireless, Mattos logged onto the website, copied PINs, and sold them to third parties without authority from Verizon. Even after Mattos left Verizon Wireless's employment in November 2003, he continued to access the website, copy PINs, and sell them to third parties. From November 2002, through March 2004, Mattos accessed the website and illegally copied over \$20 million in unused PINs.

If convicted, Mattos faces a maximum sentence of five years in prison and a fine of \$250,000, on each count of fraud in connection with computers; 20 years in prison and a fine of \$500,000, or twice the value of the laundered funds, on each count of money laundering; and 10 years in prison and a fine of \$250,000 on the count of fraud in connection with access devices. In addition, Mattos faces up to three years of supervised release on each count.

The charges are only allegations and the defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt.

###